On a type of universal forms in discretely valued fields.

By ŠTEFAN SCHWARZ in Bratislava (ČSR).

In the papers [9] and [10] I dealt with the representation of the elements of a finite field $GF(p^f)$ by the forms

$$a_1x_1^k+a_2x_2^k+\cdots+a_sx_s^k, \quad a_i\in GF(p^f).$$

I proved especially the following

Theorem 1. *Let $GF(p^f)$ be a finite field of characteristic p. Let be $\delta=(p^f-1,k)\leqq p-1$. Suppose that $a_1,a_2,\ldots,a_\delta$ are elements $\in GF(p^f)$ with $a_1a_2\ldots a_\delta\neq 0$. Then the equation*

$$a_1x_1^k+a_2x_2^k+\cdots+a_\delta x_\delta^k=b$$

has a solution with $x_1,x_2,\ldots,x_\delta\in GF(p^f)$ for every $b\in GF(p^f)$.

This theorem will be proved again as a special case of the more general Theorem 3 below.

CHEVALLEY [2] proved: If $f(x_1,x_2,\ldots,x_n)$ is any polynomial in n variables with coefficients $\in GF(p^f)$ in which the constant term is zero and if the degree of $f(x_1,x_2,\ldots,x_n)$ is less than n then

$$f(x_1,x_2,\ldots,x_n)=0$$

is soluble in $GF(p^f)$ with not all the unknowns equal to zero.

It follows from this theorem that

$$a_1x_1^k+a_2x_2^k+\cdots+a_kx_k^k-bx_{k+1}^k=0, \quad a_i,b\in GF(p^f)$$

is always (i. e. for every $k\geqq 1$) soluble with not all x_i equal to zero. But this fact does not imply that every $b\in GF(p^f)$ is representable in the form

$$b=a_1x_1^k+a_2x_2^k+\cdots+a_kx_k^k.$$

Let, for instance, $GF(7^2)$ be a field with 49 elements. We can represent all elements $\xi\in GF(7^2)$ in the form $\xi=\alpha_0+\alpha_1 j$ $(\alpha_0,\alpha_1=0,1,\ldots,6)$, where j satisfies the irreducible equation $j^2+1=0 \pmod 7$. Then the equation

$$x_1^8+x_2^8+\cdots+x_8^8-jx_9^8=0$$

is soluble in $GF(7^2)$ (f. i. with $x_1 = \cdots = x_7 = 1$, $x_8 = x_9 = 0$). But it is easy to show (see [9], p. 124) that

$$x_1^8 + x_2^8 + \cdots + x_8^8 - j = 0$$

is not soluble with $x_1, x_2, \ldots, x_8 \in GF(7^2)$. Hence the theorem of CHEVALLEY is not sharp enough to prove theorems like Theorem 1.

An other direction in which investigations have been made is the following. Let $f(x_1, \ldots, x_n)$ be a homogeneous polynomial in n variables of degree r over a p-adic number field K with integral coefficients. Then CHEVALLEY's theorem asserts that

$$f(x_1, x_2, \ldots, x_n) \equiv 0 \pmod{\mathfrak{p}}$$

has always a non-zero integral solution if $n > r$. But this does not imply that $f(x_1, x_2, \ldots, x_n) \equiv 0 \pmod{\mathfrak{p}^i}$ is soluble for every $i \geqq 1$. $f(x_1, \ldots, x_n) = 0$ need not be soluble in K.

It is known (see [1]) that to every r there exists a number $\Phi(r)$ such that if $n \geqq \Phi(r)$ $f(x_1, \ldots, x_n) = 0$ is soluble in K. HASSE [4] proved that for the quadratic case $n \geqq 5$ is sufficient. (See also JONES [5].) Recently DEMYANOV [3] and LEWIS [7] proved that, for every cubic homogeneous polynomial with $n \geqq 10$, $f(x_1, \ldots, x_n) = 0$ has in K a non-trivial solution.

For the inhomogeneous case — as far as I know — complete results are known only for quadratic forms. It holds f. i. (see JONES [5], p. 46): Let R_p be the rational p-adic field. If $f(x_1, \ldots, x_n)$ is an n-ary quadratic form with coefficients in R_p, with a non-zero determinant and $n \geqq 4$, then $f = b$ is solvable in R_p for any number b in R_p.

In this paper we shall study inhomogeneous polynomials of the form

$$a_1 x_1^k + a_2 x_2^k + \cdots + a_s x_s^k - b$$

over a field K complete under a discrete non-archimedian valuation $a_1, a_2, \ldots, a_s$, being integral elements $\in K$.

The situation is in some sense analogous to the homogeneous case mentioned above. Let, for instance, $K = R_3$ be the rational 3-adic field. The congruence $4 \equiv x_1^3 + x_2^3 + x_3^3 \pmod 3$ has solutions with integral $x_i \in R_3$. But $4 \equiv x_1^3 + x_2^3 + x_3^3 \pmod{3^2}$ has not a solution with integral $x_i \in R_3$. Hence $4 = x_1^3 + x_2^3 + x_3^3$ is not soluble with *integral* elements $\in R_3$.

We shall show that under suitable suppositions (but far not always!) the solvability of such equations can be assured by taking a sufficiently large number of summands.

There is an important remark to the example just discussed. If we admit x_1, x_2, x_3 to be any elements $\in R_3$ the equation $4 = x_1^3 + x_2^3 + x_3^3$ has in R_3 a solution. It is well known that every rational number is a sum of three

rational cubes. In our case we have f. i. $4=\left(\frac{12}{25}\right)^3+\left(\frac{47}{30}\right)^3+\left(\frac{53}{150}\right)^3$. Of course $\frac{47}{30}$ and $\frac{53}{150}$ are not integral elements $\in R_3$. This shows clearly the distinction between the solution of equations from K in integral and non necessarily integral elements $\in K$. It will be good to keep it in mind since we shall be mostly concerned (in essential) with solutions in integral elements $\in K$.

We shall use the following notations. K denotes a field, complete under a discrete non-archimedian valuation. Let I be the ring of integers $\in K$, π a local prime of K, $\mathfrak{p}=\pi I$ the prime ideal generated by π. We shall assume that the residue class field $\bar{I}=I/\mathfrak{p}$ is a finite field. The residue class containing the element $a\in I$ will be denoted by $\bar{a}$. If $f(x_1, x_2, \ldots, x_n)$ is a polynomial with coefficients in I the symbol $\bar{f}(x_1, x_2, \ldots, x_n)$ denotes the corresponding polynomial with coefficients in $\bar{I}$. (In section III the symbol $\bar{a}$ has a somewhat different meaning.)

We shall study two cases:

A. The field K has characteristic 0. It is the derived field of an algebraic number field $R(\vartheta)$ complete under a valution corresponding to a prime ideal $\mathfrak{p}$ of $J[\vartheta]$[1]), i. e. $K=R(\vartheta)_{\mathfrak{p}}$.

B. K has characteristic p. K is the field of formal power series in x (containing only a finite number of negative powers) with coefficients in a finite field $GF(p^f)$.

In both cases every element $a\in K$ is representable in the form of an infinite series (with the known definition of convergence)

$$(1)\qquad a=\frac{1}{\pi^\nu}(a_0+a_1\pi+a_2\pi^2+\cdots),\quad \nu\gtreqless 0,\ a_0\neq 0,\ a_i\in\mathfrak{R}.$$

In the case A we can choose π as an integer of the field $R(\vartheta)$ with the property $\mathfrak{p}\,\|\,\pi$, i. e. $\pi\equiv 0 \pmod{\mathfrak{p}}$ but $\pi\not\equiv 0 \pmod{\mathfrak{p}^2}$; $\mathfrak{R}$ denotes an arbitrary fixed complete system of representants of the residue classes mod $\mathfrak{p}$ containing the number 0.

In the case B we can choose π to be equal to the indeterminate x and $\mathfrak{R}$ is identified with the field $GF(p^f)$.

If in the case A $N(\mathfrak{p})=p^f$, then the residue classes $I/\mathfrak{p}$ (containing the representantes $a_i\in\mathfrak{R}$) form in both cases a field isomorphic to $GF(p^f)$.

---

[1]) $R(\vartheta)$ denotes a simple algebraic extension of the field of rational numbers R. $J[\vartheta]$ is the ring of algebraic integers $\in R(\vartheta)$.

I.

The main result of this section, in which we restrict the considerations to the case $(k, p) = 1$, is based on the Theorem 1. The proof holds in exactly the same way for both cases *A*, *B*.

Theorem 2. *Let K be a discretely valued complete field of the type A or B.*

a) Let $k > 1$ be an integer[2]*), $(k, p) = 1$.*

b) Let be $1 \leqq (k, p^f - 1) = \delta \leqq p - 1$.

c) Let $a_1, a_2, \ldots, a_{\delta+1}$ be $\delta + 1$ integral elements $\in K$, $a_1 \cdot a_2 \ldots a_{\delta+1} \not\equiv 0 \pmod{\mathfrak{p}}$.

Then every $a \in K$ can be written in the form

$$a_1 \xi_1^k + a_2 \xi_2^k + \cdots + a_{\delta+1} \xi_{\delta+1}^k, \tag{2}$$

i. e. the equation

$$a_1 x_1^k + a_2 x_2^k + \cdots + a_{\delta+1} x_{\delta+1}^k = a$$

has for every $a \in K$ a solution $\xi_1, \xi_2, \ldots, \xi_{\delta+1} \in K$.

Proof. 1. Let a be of the form (1). If $\nu > 0$ we can arrange it (by multiplication) that the number ν in the denominator is a multiple of k and has the form

$$a = \frac{1}{\pi^{lk}} (b_0 + b_1 \pi + \cdots + b_{k-1} \pi^{k-1} + b_k \pi^k + \cdots)$$

(l an integer). It is further possible to choose l so that at least one of the elements $b_0, b_1, \ldots, b_{k-1}$ is different from zero.[3]) Our theorem will be proved if we show that the element

$$b = b_0 + b_1 \pi + b_2 \pi^2 + \cdots, \qquad b_i \in \mathfrak{R}$$

can be written in the form (2).

2. In what follows we denote

$$f(\mathbf{x}) = a_1 x_1^k + a_2 x_2^k + \cdots + a_\delta x_\delta^k - b. \tag{3}$$

Let V_δ be the δ-dimensional vector space over K. A vector $\mathbf{v} = [\xi_1, \xi_2, \ldots, \xi_\delta]$, $\xi_i \in K$ will be called *primitive* if

a) $\xi_i \in I$ for every i $(1 \leqq i \leqq \delta)$,

---

[2]) The case $k = 1$ is trivial.

[3]) To this end it is sufficient to find l with the property $0 \leqq lk - \nu < k$ and to write $a = \frac{1}{\pi^{lk}} (a_0 \pi^{lk-\nu} + a_1 \pi^{lk-\nu+1} + \cdots)$.

b) there exists at least one i with $\xi_i \not\equiv 0 \pmod{\mathfrak{p}}$.

If the coordinates of the vector $\mathbf{v}$ satisfy the equation $f(\mathbf{x}) = 0$ we write $f(\mathbf{v}) = 0$.

3. Suppose first that $b \not\equiv 0 \pmod{\mathfrak{p}}$. According to Theorem 1 $\bar{f}(\mathbf{x}) = \bar{0}$ has a solution with $\bar{x}_1, \ldots, \bar{x}_n \in \bar{I}$, i. e. there exists a vector $\mathbf{v}_1 = [\xi_{11}, \xi_{21}, \ldots, \xi_{\delta 1}]$ such that $f(\mathbf{v}_1) \equiv 0 \pmod{\mathfrak{p}}$. This vector is primitive since otherwise it would be $b \equiv 0 \pmod{\mathfrak{p}}$ contrary to the supposition.

Let be $f(\mathbf{v}_1) = f(\xi_{11}, \ldots, \xi_{\delta 1}) = c \cdot \pi^m$, $m \geqq 1$, where $\pi^m \| f(\mathbf{v}_1)$ and $c \in I$. Hence $f(\mathbf{v}_1) \equiv 0 \pmod{\mathfrak{p}^m}$.

Find a vector $[\eta_1, \eta_2, \ldots, \eta_\delta]$ satisfying the relation

$$c + \sum_{i=1}^{\delta} k a_i \xi_{i1}^{k-1} \eta_i \equiv 0 \pmod{\mathfrak{p}}. \tag{4}$$

Since $c \not\equiv 0 \pmod{\mathfrak{p}}$ and for at least one i $k a_i \xi_{i1}^{k-1} \not\equiv 0 \pmod{\mathfrak{p}}$ such a vector exists. Put $\xi_{i2} = \xi_{i1} + \eta_i \pi^m$ and consider the primitive vector $\mathbf{v}_2 = [\xi_{12}, \xi_{22}, \ldots, \xi_{\delta 2}]$. It holds

$$\begin{aligned} f(\mathbf{v}_2) &= \sum_{i=1}^{\delta} a_i (\xi_{i1} + \eta_i \pi^m)^k - b = \\ &= f(\mathbf{v}_1) + \sum_{i=1}^{\delta} a_i k \xi_{i1}^{k-1} \eta_i \pi^m + \sum_{i=1}^{\delta} \binom{k}{2} \xi_{i1}^{k-2} \eta_i^2 \pi^{2m} + \cdots = \\ &= \pi^m \left[c + \sum_{i=1}^{\delta} k a_i \xi_{i1}^{k-1} \eta_i \right] + \pi^{2m} \sum_{i=1}^{\delta} \binom{k}{2} a_i \xi_{i1}^{k-2} \eta_i^2 + \cdots. \end{aligned}$$

For $l \geqq 2$ we have $lm \geqq m+1$; with respect to (4) we get

$$f(\mathbf{v}_2) \equiv 0 \pmod{\mathfrak{p}^{m+1}}.$$

This rule can be repeated. Let be $f(\mathbf{v}_2) = c' \cdot \pi^{m'}$, $m' \geqq m+1$, $\pi^{m'} \| f(\mathbf{v}_2)$ and $c' \in I$. Hence $f(\mathbf{v}_2) \equiv 0 \pmod{\mathfrak{p}^{m'}}$. Find a vector $[\zeta_1, \zeta_2, \ldots, \zeta_\delta]$ satisfying

$$c' + \sum_{i=1}^{\delta} k a_i \xi_{i2}^{k-1} \zeta_i \equiv 0 \pmod{\mathfrak{p}}.$$

Such a vector exists. Let us put $\xi_{i3} = \xi_{i2} + \zeta_i \pi^{m'}$. Then the primitive vector $\mathbf{v}_3 = [\xi_{13}, \xi_{23}, \ldots, \xi_{\delta 3}]$ satisfies the relation

$$\begin{aligned} f(\mathbf{v}_3) = \sum_{i=1}^{\delta} a_i (\xi_{i2} + \zeta_i \pi^{m'})^k - b = \pi^{m'} \left[c' + \sum_{i=1}^{\delta} k a_i \xi_{i2}^{k-1} \zeta_i \right] + \\ + \pi^{2m'} \sum_{i=1}^{\delta} \binom{k}{2} a_i \xi_{i2}^{k-2} \zeta_i^2 + \cdots, \end{aligned}$$

i. e.

$$f(\mathbf{v}_3) = 0 \pmod{\mathfrak{p}^{m'+1}}.$$

By this rule a sequence of primitive vectors $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \ldots$ can be found such that $f(\mathbf{v}_i) \equiv 0 \pmod{\mathfrak{p}^{m+i}}$.

Since the ring I and the set of integral elements of K which are $\not\equiv 0 \pmod{\mathfrak{p}}$ are both compact there exists a subsequence of the sequence $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \ldots$ which converges to a primitive vector $\mathbf{v} = [\xi_1, \xi_2, \ldots, \xi_\delta]$. (By the convergence of a sequence of vectors we mean here the componentwise convergence.) Since $f(\mathbf{x})$ is a continuous function we get $f(\mathbf{v}) = 0$. Our theorem in the case $b \not\equiv 0 \pmod{\mathfrak{p}}$ is proved even with the sharper result that we can choose $x_{\delta+1} = 0$.

4. Let be $b \equiv 0 \pmod{\mathfrak{p}}$. The rule just applied cannot be used since Theorem 1 does not assure the existence of a primitive vector $\mathbf{v}_1$ satisfying $f(\mathbf{v}_1) \equiv 0 \pmod{\mathfrak{p}}$.

Consider therefore the element $d = b - a_{\delta+1}$. Since $d \not\equiv 0 \pmod{\mathfrak{p}}$ there exists a primitive vector $\mathbf{v} = [\xi_1, \ldots, \xi_\delta]$ such that

$$b - a_{\delta+1} = a_1 \xi_1^k + \cdots + a_\delta \xi_\delta^k.$$

Hence it is

$$b = a_1 \xi_1^k + \cdots + a_\delta \xi_\delta^k + a_{\delta+1} \cdot 1^k.$$

Theorem 2 is completely proved.

It follows from the proof of Theorem 2 and the remark under 4 above the validity of the following

Theorem 2a. *Let the suppositions of Theorem 2 be satisfied with the modification that we have only δ integral elements $a_1, a_2, \ldots, a_\delta \in K$, where $a_1 \cdot a_2 \cdots a_\delta \not\equiv 0 \pmod{\mathfrak{p}}$. Then, if the congruence*

$$a_1 x_1^k + \cdots + a_\delta x_\delta^k \equiv 0 \pmod{\mathfrak{p}}$$

has at least one non-zero solution, then every element $b \in K$ can be written in the form

$$b = a_1 \xi_1^k + \cdots + a_\delta \xi_\delta^k, \quad \xi_i \in K.$$

Remark 1. The result of Theorem 2 is sharp in the sense that, in general, the number $\delta + 1$ cannot be replaced by a less one. We show this on an example in the rational p-adic field R_p.

Choose $p = 7$, $k = 2$ (hence $\delta = 2$) and $a_1 = a_2 = a_3 = 1$. According to Theorem 2 every $a \in R_7$ can be written in the form

$$a = \xi_1^2 + \xi_2^2 + \xi_3^2, \xi_i \in R_7.$$

But it is not true that $a = 7$ can be written in the form

$$7 = \xi_1^2 + \xi_2^2. \tag{5}$$

We show first that if (5) holds then ξ_1, ξ_2 are necessarily integral elements $\in R_7$. Let be

$$\xi_1 = \frac{1}{7^\mu}(\xi_{10} + \xi_{11}\cdot 7 + \xi_{12}\cdot 7^2 + \cdots),\ \xi_{10} \neq 0,$$

$$\xi_2 = \frac{1}{7^\nu}(\xi_{20} + \xi_{21}\cdot 7 + \xi_{22}\cdot 7^2 + \cdots),\ \xi_{20} \neq 0,$$

$\xi_{ik} \in \mathfrak{R}$, $\mathfrak{R} = \{0, 1, \ldots, 6\}$, $\mu > 0$, $\nu > 0$. Without loss of generality suppose $\mu \geqq \nu$.[4]) The condition (5) implies

$$7 = \frac{1}{7^{2\mu}}(\xi_{10} + \cdots)^2 + \frac{1}{7^{2\nu}}(\xi_{20} + \cdots)^2, \tag{6}$$

i. e.

$$7^{2\mu+1} - (\xi_{10} + \cdots)^2 - 7^{2(\mu-\nu)}\cdot(\xi_{20} + \cdots)^2 = 0.$$

If $\mu - \nu > 0$ there would be $\xi_{10} \equiv 0 \pmod 7$, contrary to the assumption. If $\mu - \nu = 0$ we get $\xi_{10}^2 + \xi_{20}^2 \equiv 0 \pmod 7$, which can be satisfied only with $\xi_{10} = \xi_{20} = 0$, again contrary to the supposition.

Now, we show that there cannot exist integral elements

$$\xi_i = \xi_{i0} + \xi_{i1}\cdot 7 + \xi_{i2}\cdot 7^2 + \cdots, \quad \xi_{ik} \in \mathfrak{R} \quad (i = 1, 2)$$

satisfying (5). Substituting in (5) we get $\xi_{10}^2 + \xi_{20}^2 \equiv 0 \pmod 7$. This implies $\xi_{10} = \xi_{20} = 0$. But then (5) gives

$$7 = (7\xi_{11} + \cdots)^2 + (7\xi_{21} + \cdots)^2,$$

i. e. $7 \equiv 0 \pmod{7^2}$, what is impossible.

Remark 2. It follows from the proof of Theorem 2 that under the suppositions *a*)—*c*) every integral element $\in K$ can be written in the form (2) with integral $\xi_1, \ldots, \xi_{\delta+1} \in K$.

We show on an example that in the representation of an integral element $a \in K$ by means of integral $\xi_1, \ldots, \xi_{\delta+1} \in K$ the condition $(k, p^f - 1) \leqq p - 1$ cannot be replaced by a less sharp condition.[5])

Let K be the derived field of the Gaussian field $R(i)$ complete under the p-adic valuation, where $\mathfrak{p} = [7]$. We have $N(\mathfrak{p}) = 7^2$. Choose $k = 8$; then $\delta = (8, 7^2 - 1) = 8 > 6$. We can take $\pi = 7$. Every integral element $\in K$ is of the form

$$\xi = \xi_0 + \xi_1\cdot 7 + \xi_2\cdot 7^2 + \cdots \qquad \xi_i \in \mathfrak{R},$$

---

[4]) If $\mu > 0$ then we have also $\nu > 0$. For $\mu > 0, \nu \leqq 0$ would imply that the right hand side of (6) is a non-integral element $\in R_7$, whereas the left hand side is clearly an integral element $\in R_7$.

[5]) It remains open whether the condition $(k, p^f - 1) \leqq p - 1$ can be replaced by a less sharp if we admit for $\xi_1, \ldots, \xi_{\delta+1}$ any numbers $\in K$.

where $\mathfrak{R}$ denotes f. i. the numbers $a+bi$ $(a, b=0, 1, \ldots, 6)$. We show that it is not possible to write $i \in K$ as a sum of eighth powers of integral elements $\in K$. The relation

$$i=\sum_{k=1}^{s}(\xi_{0k}+\xi_{1k}\cdot 7+\xi_{2k}\cdot 7^2+\cdots)^8,\ \xi_{ik}\in\mathfrak{R},$$

would imply

$$i\equiv\sum_{k=1}^{s}\xi_{0k}^8 \pmod{[7]}. \tag{7}$$

But for every number $a+bi$ it holds

$$(a+bi)^8=a^8+8a^7bi+\cdots+8ab^7i^7+b^8\equiv a^8+b^8+abi(a^6-b^6) \pmod{[7]}.$$

If at least one of the numbers a, b is equal to zero we have $ab\equiv 0 \pmod{[7]}$. If $a\not\equiv 0, b\not\equiv 0$ we have $a^6-b^6\equiv 1-1=0 \pmod{[7]}$. In both cases we have therefore

$$\xi_{ik}^8=(a_k+ib_k)^8\equiv a_k^8+b_k^8\equiv a_k^2+b_k^2 \pmod{[7]}.$$

The relation (7) implies

$$i\equiv\sum_{k=1}^{s}(a_k^2+b_k^2) \pmod{[7]},$$

what is impossible, since a number of the form $\frac{1}{7}\left[i-\sum_{k=1}^{s}(a_k^2+b_k^2)\right]$ is not an algebraic integer of the field $R(i)$.

Remark 3. Let $K=R_p$ be the rational p-adic field. Suppose $p>2$. If we apply the result of Theorem 2 and 2a to the case $k=2$ we get well-known results concerning quadratic forms. Let a_1, a_2, a_3 be arbitrary integral elements $\in R_p$, $a_1a_2a_3\not\equiv 0 \pmod p$.[6]) Every number $a\in R_p$ can be written in the form

$$a=a_1\xi_1^2+a_2\xi_2^2+a_3\xi_3^2.$$

For every integral $b\not\equiv 0 \pmod p$ and arbitrary integral $a_1, a_2\in R_p$ with $a_1a_2\not\equiv 0 \pmod p$ it is even possible to writte $b=a_1\xi_1^2+a_2\xi_2^2$, $\xi_i\in R_p$.

These and analogous results concerning quadratic forms are treated in detail in the book of B. W. JONES [5].

---

[6]) The condition $a_1a_2a_3\not\equiv 0 \pmod p$ cannot be replaced by the weaker condition $a_1a_2a_3\neq 0$, since for instance the equation $6=x_1^2+x_2^2+3x_3^2$ is not soluble in R_3 with integral $x_1, x_2, x_3\in R_3$.

II.

In theorem 2 we supposed nothing about the characteristic of the field K (i. e. there was not necessary to distinguish between the cases A and B). But it was of course essential that $(k, p) = 1$. The difficulties which made impossible to prove Theorem 1 in the case $(k, p) > 1$ are clearly to see for instance in the equation (4) since this equation reduces in this case to a contradiction $c \equiv 0 \pmod{\mathfrak{p}}$.

In the following we shall give a full discussion of the case $(k, p) \geqq 1$. Write $k = k_0 p^t$, $(k_0, p) = 1$, $t \geqq 0$.

The case B, where the fields K and $l/\mathfrak{p}$ have both characteristic p, can be settled at once.

Suppose $t > 0$. Let $a_1, a_2, \ldots, a_s$ be integral elements $\in K$. The equation

$$a = a_1 \xi_1^k + \cdots + a_s \xi_s^k \tag{8}$$

need not have for any $s > 0$ a solution with $\xi_1, \xi_2, \ldots, \xi_s \in K$.[7])

Every element $a \in K$ can be written in the form of a formal power series in the indeterminate x

$$a = a_{-r} x^{-r} + a_{-r+1} x^{-r+1} + \cdots + a_0 + a_1 x + a_2 x^2 + \cdots,$$

$a_i \in \mathfrak{R} = GF(p^f) \cong l\,[x]$. The k-th power of $a \in K$ is of the form

$$a^k = (a_{-r} x^{-r} + \cdots + a_0 + a_1 x + \cdots)^{k_0 p^t} =$$
$$= [a_{-r}^{p^t} \cdot x^{-rp^t} + a_{-r+1}^{p^t} x^{(-r+1)p^t} + \cdots + a_0^{p^t} + a_1^{p^t} x^{p^t} + a_2^{p^t} \cdot x^{2p^t} + \cdots]^{k_0}.$$

We show easily that the element x cannot be written as a sum of k-th powers of elements $\in K$.[8]) For if it were

$$x = \sum_{i=1}^{s} \xi_i^k = \sum_{i=1}^{s} [x^{-r_i} (\xi_{i0} + \xi_{i1} x + \xi_{i2} x^2 + \cdots)]^k, \qquad \xi_{il} \in \mathfrak{R}$$

it would hold also

$$x = \sum_{i=1}^{s} [x^{-r_i p^t} (\xi'_{i0} + \xi'_{i1} x^{p^t} + \xi'_{i2} x^{2p^t} + \cdots)]^{k_0},$$

where $\xi'_{il} = \xi_{il}^{p^t}$. Without loss of generality suppose $r_1 \geqq r_2 \geqq \cdots \geqq r_s$. We have

$$x^{r_1 k_0 p^t + 1} = (\xi'_{10} + \xi'_{11} x^{p^t} + \cdots)^{k_0} + x^{(r_1 - r_2) k_0 p^t} (\xi'_{11} + \xi'_{12} x^{p^t} + \cdots)^{k_0} + \cdots +$$
$$+ x^{(r_1 - r_s) k_0 p^t} (\xi'_{1s} + \xi'_{2s} x^{p^t} + \cdots)^{k_0}.$$

---

[7]) Independently of the fact whether $(k, p^f - 1) \leqq p - 1$ holds or not.

[8]) I. e. we put in (8) $a_1 = a_2 = \cdots = a_s = 1$.

Hence (since clearly ν_1 must be $\geqq 0$)

$$(9) \qquad x^{\nu_1 k_0 p^t+1} \equiv \eta_0 + \eta_1 x^{p^t} + \eta_2 x^{2p^t} + \cdots + \eta_{\nu_1 k_0} x^{\nu_1 k_0 p^t} \pmod{x^{(\nu_1 k_0+1)p^t}}$$

with some $\eta_1, \eta_2, \ldots, \eta_{\nu_1 k_0} \in \mathfrak{R}$.

Since $t \geqq 1, p \geqq 2$, we have $p^t \geqq 2$. On the right hand side of the equation (9) we have a polynomial in x^{p^t}. But the exponent $\nu_1 k_0 p^t + 1$ on the left hand side of (9) is clearly not divisible by p^t. Such a relation is impossible and our assertion is proved.

III.

In the following we shall restrict the considerations to the case of a derived field of an algebraic number field $R(\vartheta)$, complete under a p-adic valuation. This field will be denoted by $K = R(\vartheta)_\mathfrak{p}$. The symbol $J[\vartheta]$ denotes the ring of algebraic integers of the field $R(\vartheta)$.

We prove a series of lemmas with the final aim to prove a theorem analogous to Theorem 1 dealing with the finite ring $J[\vartheta]/\mathfrak{p}^{t+1}$ instead of the finite field $J[\vartheta]/\mathfrak{p}$.

Lemmas 1—3 which are well-known in the theory of algebraic numbers are quoted without proofs. (They can be found for instance in O. Ore [8], pp. 51—61.)

Throughout all this section let further be $N(\mathfrak{p}) = p^f$, $f \geqq 1$, $p \geqq 2$.[9]) The polynomial

$$(10) \qquad \varphi(x) = x^f + a_1 x^{f-1} + \cdots + a_f$$

denotes an arbitrary (fixed chosen) polynomial of degree f with rational integral coefficients and leading coefficient 1 irreducible (mod p).

Lemma 1. *The congruence*

$$(11) \qquad \varphi(x) \equiv x^f + a_1 x^{f-1} + \cdots + a_f \equiv 0 \pmod{\mathfrak{p}}$$

has just f (mod $\mathfrak{p}$) *distinct solutions* $\in J[\vartheta]$. *If one of the solutions is the number* $\alpha \in J[\vartheta]$, *then the numbers* $\alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{f-1}}$ *are the remaining solutions of* (11).

Lemma 2. *If* $\alpha \in J[\vartheta]$ *is an arbitrary fixed chosen solution of* (11), *then the numbers*

$$(12) \qquad C(\alpha) = c_0 + c_1\alpha + \cdots + c_{f-1}\alpha^{f-1}$$

($c_i = 0, 1, \ldots, p-1$) *form a complete system of representants of the residue classes* (mod $\mathfrak{p}$).

---

[9]) The restriction $p \geqq 3$ will not be necessary until we treat Theorem 4.

Remark. If $f=1$, the number α does not appear, of course, explicitly in (12).

Lemma 3. *Let π be an algebraic number $\in J[\mathfrak{P}]$ for which $\mathfrak{p}\|\pi$ holds. Let u be an integer, $u \geqq 0$. Then a complete set of representants of the residue classes* (mod $\mathfrak{p}^{u+1}$) *is given by the following $p^{f(u+1)} = N(\mathfrak{p})^{u+1}$* (mod $\mathfrak{p}^{u+1}$ *incongruent) numbers:*

$$C_0(\alpha) + C_1(\alpha)\cdot\pi + \cdots + C_u(\alpha)\cdot\pi^u. \tag{13}$$

Here $\alpha \in J[\mathfrak{P}]$ is defined as a solution of the congruence (11) *and the set $C_i(\alpha)$ has a meaning which is clear from the Lemma* 2.

Remark: If $\mathfrak{p}\|p$ we can choose $\pi = p$.

Till to the end of the paper we shall use the following notations. Let be $k = k_0 p^t, (k_0, p) = 1$, $t \geqq 0$. Put $\delta = (k_0, p^f - 1)$. The symbol Z denotes the ring of residue classes (mod $\mathfrak{p}^{t+1}$). The symbol Z_0 denotes the set of non-zero residue classes (mod $\mathfrak{p}^{t+1}$). The symbol Z^* denotes the group of residue classes (mod $\mathfrak{p}^{t+1}$) which are relatively prime to $\mathfrak{p}$.[10]) Finally the symbol $Z^{(k)}$ denotes the set of all non-zero residue classes (mod $\mathfrak{p}^{t+1}$) which are k-th powers of residue classes (mod $\mathfrak{p}^{t+1}$).

The elements of the sets $Z, Z_0, Z^*, Z^{(k)}$ are classes mod $\mathfrak{p}^{t+1}$. The class whose representant is the number n will be denoted by $\overline{n}$.

Lemma 4. Let be $k>1$, $k=k_0 p^t$, $(k_0, p)=1$, $\mathfrak{p}|p$, $\mathfrak{p}\|\pi$. *Denote* $\lambda = \binom{k}{l}\pi^{l\varrho}$, *where l, ϱ are integers $\geqq 1$. Then,*

a) for $p \geqq 2$, $1 \leqq l \leqq k$, we have $\mathfrak{p}^{t+1}|\lambda$;
b) for $p \geqq 3$, $2 \leqq l \leqq k$, we have $\mathfrak{p}^{t+2}|\lambda$;
c) for $p \geqq 2$, $\varrho > 1$, $2 \leqq l \leqq k$, we have $\mathfrak{p}^{t+\varrho+1}|\lambda$;
d) for $p=2$, $l \geqq 3$, we have $\mathfrak{p}^{t+2}|\lambda$.

Proof. Let us put $l = l_0 \cdot p^\tau$, $(l_0, p) = 1$, where $1 \leqq \tau \leqq t$. Then[11])

$$\lambda = \binom{k}{l}\pi^{l\varrho} = \frac{k}{l}\binom{k-1}{l-1}\pi^{l\varrho} = \frac{k_0}{l_0}\binom{k-1}{l-1}p^{t-\tau}\pi^{l_0\varrho p^\tau}.$$

Therefore λ is divisible by $\mathfrak{p}^\sigma$, where $\sigma \geqq m = t + l_0\varrho p^\tau - \tau$.

In the case *a*) : $m \geqq t + 2^\tau - \tau \geqq t+1$.

In the case *b*) : $m \geqq t + l_0 p^\tau - \tau = t + l - \tau$. If $\tau = 0$, we have $m \geqq t + l \geqq t+2$. If $\tau > 0$, we have $m \geqq t + 3^\tau - \tau \geqq t+2$.

The case *c*). If $\tau = 0$, we have $m = t + l\varrho - \tau = t + l\varrho \geqq t + 2\varrho \geqq t + \varrho + 1$. If $\tau \geqq 1$, we have $m \geqq t + 1\cdot 2^\tau \cdot \varrho - \tau \geqq t + 2\varrho - 1 \geqq t + \varrho + 1$.

---

[10]) Let us recall that the group Z^* is — in general — not cyclic.

[11]) The symbol $\binom{k-1}{0}$ denotes 1.

The case *d*). If $\tau=0$, we have $m=t+l\varrho\geqq t+3$. If $\tau>0$ and it holds $l=l_0\cdot 2^\tau\geqq 3$, then we have α) either $\tau=1$, $l_0\geqq 3$, β) or $\tau\geqq 2$. In the case α) we have $m\geqq t+l_0p^\tau-\tau=t+3\cdot 2-1=t+5$. In the case β) we get $m\geqq t+l_0 2^2-2\geqq t+2$.

This proves Lemma 4.

Lemma 5. *Let α,β be two numbers $\in J[\vartheta]$. Then $\alpha\equiv\beta$ (mod p) implies $\alpha^{p^t}\equiv\beta^{p^t}$ (mod p^{t+1}).*

Proof: Well-known.

Lemma 6. *We find all elements of the set $Z^{(k)}$ among the classes which are represented by the numbers*

$$[c_0+c_1\alpha+\cdots+c_{f-1}\alpha^{f-1}]^k \qquad (\text{mod } p^{t+1})$$

($c_i=0,1,\ldots,p-1$). Among these classes there exist precisely $\frac{p^f-1}{\delta}$ non-zero distinct classes. Each of these non-zero classes (mod p^{t+1}) *is at the same time a non-zero class* (mod p)[12])

Proof. With respect to (12) the representant of every class $\bar{\omega}\in Z^{(k)}$ can be written in the form

$$\begin{aligned}\omega&\equiv[C_0(\alpha)+C_1(\alpha)\cdot\pi+\cdots+C_t(\alpha)\cdot\pi^t]^k=\\&\equiv[C_0(\alpha)+\pi\cdot D(\alpha)]^k, \qquad (\text{mod } p^{t+1}),\end{aligned}$$

where

$$D(\alpha)=C_1(\alpha)+C_2(\alpha)\cdot\pi+\cdots+C_t(\alpha)\,\pi^{t-1}.$$

Hence it is

$$\omega\equiv C_0(\alpha)^k+\sum_{i=1}^{k}\binom{k}{i}\pi^i C_0(\alpha)^{k-i}D(\alpha)^i. \tag{14}$$

According to Lemma 4a every member of the second summand in (14) is $\equiv 0$ (mod p^{t+1}), i. e.

$$\omega\equiv C_0(\alpha)^k=(c_0+c_1\alpha+\cdots+c_{f-1}\alpha^{f-1})^{k_0p^t} \qquad (\text{mod } p^{t+1}).$$

This proves the first assertion of Lemma 6.

We wish to establish now how many among the numbers

$$[c_0+c_1\alpha+\cdots+c_{f-1}\alpha^{f-1}]^k,\ 0\leqq c_i\leqq p-1 \tag{15}$$

are distinct (mod p^{t+1}).

---

[12]) This means: among the numbers which are not relatively prime to p only the number 0 is a *k*-th power (mod p^{t+1}). This is in general not true for *k*-th power residues (mod p^{t+2}). For instance: take in the field of rational numbers $k=2$, $p=2$. Then the quadratic residues (mod 8) are the numbers 0, 1, 4. Here 4 is divisible by $p=2$. Hence the squares $\neq 0$ do not form a group.

Let us establish first how many of the numbers (15) are different (mod $\mathfrak{p}$). We have clearly

$$\omega = [c_0 + c_1\alpha + \cdots + c_{f-1}\alpha^{f-1}]^{k_0 p^t} \equiv [c_0 + c_1\alpha^{p^t} + c_2\alpha^{2p^t} + \cdots + c_{f-1}\alpha^{(f-1)p^t}]^{k_0} \pmod{\mathfrak{p}}.$$

According to Lemma 1 the number $\alpha^{p^t} = \beta$ is one of the solutions of the congruence (11). Write

$$\omega \equiv (c_0 + c_1\beta + c_2\beta^2 + \cdots + c_{f-1}\beta^{f-1})^{k_0} \pmod{\mathfrak{p}} \tag{16}$$

The non-zero classes (mod $\mathfrak{p}$) form a cyclic group of order $p^f - 1$. The classes which are k_0-th powers form a subgroup of index $\delta = (k_0, p^f - 1)$. Hence among the classes represented by the numbers (15) there exist just $\frac{p^f - 1}{\delta}$ non-zero different classes (mod $\mathfrak{p}$). Therefore there exist at least $\frac{p^f - 1}{\delta}$ different classes (mod $\mathfrak{p}^{t+1}$).

The symbol $\omega(\omega', \omega'')$ denotes in the following numbers belonging to the set (15). We shall show that even (mod $\mathfrak{p}^{t+1}$) there exist among the numbers (15) exactly $\frac{p^f - 1}{\delta}$ different numbers. To this end it is sufficient to prove that $\omega' \equiv \omega''$ (mod $\mathfrak{p}$) implies $\omega' \equiv \omega''$ (mod $\mathfrak{p}^{t+1}$).

Let be

$$\omega' = (c_0' + c_1'\alpha + \cdots + c_{f-1}'\alpha^{f-1})^k \equiv \omega'' = (c_0'' + c_1''\alpha + \cdots + c_{f-1}''\alpha^{f-1})^k \pmod{\mathfrak{p}}, \tag{17}$$

i. e.

$$\omega' \equiv (c_0' + c_1'\beta + \cdots + c_{f-1}'\beta^{f-1})^{k_0} \equiv \omega'' \equiv (c_0'' + c_1''\beta + \cdots + c_{f-1}''\beta^{f-1})^{k_0} \pmod{\mathfrak{p}}, \tag{18}$$

where $\beta = \alpha^{p^t}$.

According to FERMAT's theorem $\alpha \equiv \alpha^{p^f} \equiv \alpha^{p^{2f}} \equiv \alpha^{p^{3f}} \equiv \cdots \pmod{\mathfrak{p}}$. Let r be an integer such that $rf < t \leqq (r+1)f$. Raise (18) to the power $\nu = p^{(r+1)f - t}$. Since $\beta^\nu \equiv \alpha^{\nu p^t} \equiv \alpha^{p^{(r+1)f}} \equiv \alpha \pmod{\mathfrak{p}}$ and $c_i^\nu \equiv c_i \pmod{\mathfrak{p}}$ we get

$$(c_0' + c_1'\alpha + \cdots + c_{f-1}'\alpha^{k-1})^{k_0} \equiv (c_0'' + c_1'' + \cdots + c_{f-1}''\alpha^{f-1})^{k_0} \pmod{\mathfrak{p}}.$$

If we denote

$$\lambda' = (c_0' + c_1'\alpha + \cdots + c_{f-1}'\alpha^{f-1})^{k_0},$$
$$\lambda'' = (c_0'' + c_1''\alpha + \cdots + c_{f-1}''\alpha^{f-1})^{k_0},$$

we get

$$\lambda' \equiv \lambda'' \pmod{\mathfrak{p}} \tag{19}$$

According to Lemma 5 it follows from (19)

$$\lambda'^{p^t} \equiv \lambda''^{p^t} \pmod{\mathfrak{p}^{t+1}},$$

i. e.

$$(c_0'+c_1'\alpha+\cdots+c_{f-1}'\alpha^{f-1})^k\equiv(c_0''+c_1''\alpha+\cdots+c_{f-1}''\alpha^{f-1})^k \pmod{\mathfrak{p}^{t+1}}$$

$$\omega'\equiv\omega'' \pmod{\mathfrak{p}^{t+1}}. \tag{20}$$

This proves Lemma 6.

The numbers (15) (with exception of zero) are not divisible by $\mathfrak{p}$. This remark enables to prove at once the following

Lemma 7. a) *The set $Z^{(k)}$ forms a group, $Z^{(k)}\subset Z^{(*)}$.* b) *For the index $[Z^*:Z^{(k)}]$ we have $[Z^*:Z^{(k)}]=p^{ft}\cdot\delta$.*

Proof. The statement a) is clear from the precedent. The order of the group Z^* is

$$\varphi(\mathfrak{p}^{t+1})=N(\mathfrak{p}^{t+1})\left(1-\frac{1}{N(\mathfrak{p})}\right)=p^{ft}(p^f-1).$$

According to Lemma 6 the order of the group $Z^{(k)}$ is $\frac{p^f-1}{\delta}$. Hence

$$\text{index}\,[Z^*:Z^{(k)}]=p^{ft}(p^f-1):\frac{p^f-1}{\delta}=p^{ft}\cdot\delta.$$

Lemma 8. *Let $\bar{n}\neq\bar{0}$ be an arbitrary element $\in Z$. Every complex $\bar{n}Z^{(k)}$ contains precisely $\frac{p^f-1}{\delta}$ different elements.*

Remark. The set Z (with respect to multiplication) is not a group, merely a semigroup. For $\bar{n}\in Z^*$ the assertion of the Lemma is an elementary fact of the theory of groups (since $Z^{(k)}$ is a subgroup of Z^*). It is important that the lemma holds also for $\bar{n}\in Z-Z^*$.

Proof. Let $\bar{\xi}^k, \bar{\eta}^k$ be two elements $\in Z^{(k)}$. It is sufficient to prove: if $\bar{n}$ is a non-zero class (mod $\mathfrak{p}^{t+1}$), then

$$n\bar{\xi}^k\equiv n\eta^k \pmod{\mathfrak{p}^{t+1}} \quad\text{implies}\quad \bar{\xi}^k\equiv\eta^k \pmod{\mathfrak{p}^{t+1}}.$$

Let be $\mathfrak{p}^j\|[n]$, $0\leqq j<t+1$. Then $\mathfrak{p}^{t+1}\mid n(\bar{\xi}^k-\eta^k)$ implies $\mathfrak{p}^{t+1-j}\mid\bar{\xi}^k-\eta^k$, i. e. $\bar{\xi}^k\equiv\eta^k \pmod{\mathfrak{p}^{t+1-j}}$. The more there is therefore

$$\bar{\xi}^k\equiv\eta^k \pmod{\mathfrak{p}}. \tag{21}$$

In the same manner as we deduced (20) from (17) we can deduce from (21) $\bar{\xi}^k\equiv\eta^k \pmod{\mathfrak{p}^{t+1}}$. This proves Lemma 8.

Lemma 9. *Two complexes $\bar{n}_1Z^{(k)}, \bar{n}_2Z^{(k)}, \bar{n}_1, \bar{n}_2\in Z$ ($\bar{n}_1, \bar{n}_2$ non-zero classes) are either disjoint or iaentical.*

Proof. Suppose that the intersection is non vacuous, i. e. there exist two elements $\bar{\xi}^k, \bar{\eta}^k\in Z^{(k)}$ such that $\bar{n}_1\bar{\xi}^k=\bar{n}_2\bar{\eta}^k$, i. e. $n_1\bar{\xi}^k\equiv n_2\eta^k \pmod{\mathfrak{p}^{t+1}}$. Since $\bar{\xi}^k\in Z^*$, there exists an element $\bar{\xi}_1^k\in Z^*$ such that $\bar{\xi}^k\bar{\xi}_1^k\equiv 1 \pmod{\mathfrak{p}^{t+1}}$.

Hence we have $n_1 \equiv n_2(\xi_1\eta_1)^k \pmod{\mathfrak{p}^{t+1}}$. Therefore $\overline{n}_1 Z^{(k)} = \overline{n}_2(\overline{\eta_1\xi_1})^k Z^{(k)} = \overline{n}_2 Z^{(k)}$, which proves the lemma.

A corollary of the lemmas proved above is the

Lemma 10. *The ring Z of residue classes* $\pmod{\mathfrak{p}^{t+1}}$ *is a sum of* $\frac{p^{f(t+1)}-1}{p^f-1}\delta+1$ *disjoint complexes of the form* $\overline{n}Z^{(k)}$. *One of the complexes contains a single element* 0, *every of the remaining complexes contains exactly* $\frac{p^f-1}{\delta}$ *elements.*

Therefore it is possible to write the ring Z (in a unique way) as a sum of disjoint summands

$$Z = \overline{0} + \overline{n}_1 Z^{(k)} + \overline{n}_2 Z^{(k)} + \cdots + \overline{n}_s Z^{(k)}, \tag{22}$$

where $\overline{n}_1 = \overline{1}$, $\overline{n}_i \in Z$, $s = \frac{p^{f(t+1)}-1}{p^f-1}\delta$.

In lemmas 11 and 12 we shall prove the possibility to choose the number $\alpha \in J[\mathfrak{P}]$ in a special way which turns out to be essential for the proof of Theorem 3.

Lemma 11. *Let be $f \geqq 1$, $\delta = (k_0, p^f-1) \leqq p-1$. Then there exists a polynomial $\varphi(x)$ irreducible* $\pmod p$ *of degree f which divides* $\pmod p$ *the polynomial*

$$x^{\frac{p^f-1}{\delta}} - 1. \tag{23}$$

Proof.[13]) Let be $f > 1$. Every irreducible polynomial $\pmod p$ of degree f divides

$$x^{p^f-1} - 1. \tag{24}$$

The polynomial (23) divides the polynomial (24). We shall show that the sum of degrees of all irreducible polynomials dividing (23) with a degree $< f$ is less than the number $\frac{p^f-1}{\delta}$. This will prove Lemma 11. For, first (23) has not $\pmod p$ factors of degree $> f$, secondly the sum of degrees of all $\pmod p$ irreducible polynomials dividing (23) is exactly $\frac{p^f-1}{\delta}$. Hence (23) has at least one factor of degree f.

The polynomial (23) has only irreducible factors of a degree d, where d/f. Such an irreducible factor of degree d divides $x^{p^d}-x$. Therefore the sum

[13]) See [9], p. 125. For $f=1$ the lemma is trivial.

of degrees of all irreducible factors of degree d is at most p^d. The sum of degrees of all irreducible factors of (23) of degree $<f$ is less then the number

$$\sigma = \sum_{d,f,\, d<f} p^d.$$

Hence

$$\sigma \leqq \sum_{d=1}^{f-1} p^d < 1 + \sum_{d=1}^{f-1} p^d = \frac{p^f-1}{p-1} \leqq \frac{p^f-1}{\delta},$$

i. e. $\sigma < \frac{p^f-1}{\delta}$ This proves our Lemma.

Lemma 12. *The number α in Lemma 2 (or 3) can be chosen in such a manner that*

$$\alpha \equiv \beta^k \pmod{\mathfrak{p}^{t+1}},$$

where $\beta \in J[\vartheta]$.

Proof. Let us choose for the polynomial (11) such an irreducible polynomial $\varphi(x)$ of degree f which divides (23) According to Lemma 11 this is possible. The root $\alpha_1 \in J[\vartheta]$ of the congruence

$$\varphi(x) \equiv x^f + a_1 x^{f-1} + \cdots + a_f \equiv 0 \pmod{\mathfrak{p}} \tag{25}$$

satisfies the more the congruence

$$x^{\frac{p^f-1}{\delta}} - 1 \equiv 0 \pmod{\mathfrak{p}}.$$

We have therefore

$$\alpha_1^{\frac{N(\mathfrak{p})-1}{\delta}} \equiv 1 \pmod{\mathfrak{p}}, \quad \delta = (k_0, N(\mathfrak{p})-1). \tag{26}$$

It is well-known that (26) is satisfied by those and only those numbers $\alpha_1 \in J[\vartheta]$ which are k_0-th powers (mod $\mathfrak{p}$), i. e. for which

$$\alpha_1 \equiv \beta^{k_0} \pmod{\mathfrak{p}} \tag{27}$$

holds. Hence every solution of (25) is a k_0-th power (mod $\mathfrak{p}$). According to Lemma 5 it follows from (27)

$$\alpha_1^{p^t} \equiv \beta^{k_0 p^t} = \beta^k \pmod{\mathfrak{p}^{t+1}}.$$

The number $\alpha_1^{p^t}$ is simultaneously with α_1 a solution of (25). Denoting $\alpha = \alpha_1^{p^t}$ we get

$$\alpha \equiv \beta^k \pmod{\mathfrak{p}^{t+1}},$$

which proves our Lemma.

Lemmas 1—12 hold independently whether $\mathfrak{p} \| p$ or only $\mathfrak{p} | p$. From now on suppose explicitly $\mathfrak{p} \| p$. Then in Lemma 3 we can write p instead of π. Hence the residue classes belonging to Z are just represented by the numbers

$$C_0(\alpha) + C_1(\alpha) p + \cdots + C_t(\alpha) \cdot p^t. \tag{28}$$

By rearranging this expression we see that every number from (28) can be written in the form

$$d_0+d_1\alpha+d_2\alpha^2+\cdots+d_{f-1}\alpha^{f-1},$$

where d_i are rational integers. This implies the validity of the following Lemma

Lemma 13. *Let be $\mathfrak{p}\|p$. Then every element $\in Z$ can be represented by just one of the numbers*

$$\xi=d_0+d_1\alpha+\cdots+d_{f-1}\alpha^{f-1}, \tag{29}$$

where d_i runs through all numbers $0, 1, 2, \ldots, p^{t+1}-1$.

From now (till to the end of this paper) we shall choose the representants of the classes $\in Z$ exclusively from the set (29). Thus the representant is uniquely determined.

We introduce two notions. The numbers $(d_0, d_1, \ldots, d_{f-1})$ will be called the *coordinates* of the element ξ, the number of coordinates different from zero will be called the *length* of the element ξ. If $\xi\neq 0$ the length l is an integer, $1\leqq l\leqq f$.

Choose the number α in Lemma 13 so that $\alpha\equiv\beta^k \pmod{\mathfrak{p}^{t+1}}$. Then it holds

Lemma 14. *Let $\overline{\xi n}\cdot Z^{(k)}$ be a non-zero complex, ξ of the length l. Then there exists a number η of the same length l having the first coordinate $d_0\neq 0$ and satisfying the relation*

$$\overline{\xi n}\cdot Z^{(k)}=\overline{\eta n}\cdot Z^{(k)}.$$

Proof. a) If $f=1$ the assertion is trivial, since the representant of every non-zero complex has the first (and only first) coordinate $\neq 0$.

b) Suppose $f>1$ and $\xi=d_\varrho\alpha^\varrho+d_{\varrho+1}\alpha^{\varrho+1}+\cdots+d_{f-1}\alpha^{f-1}$ $(d_\varrho\neq 0,\ \varrho\geqq 1)$. Since α and therefore $\alpha^\varrho, \alpha^{-\varrho}$ are k-th powers $(\bmod \mathfrak{p}^{t+1})$ we have $\overline{\alpha}, \overline{\alpha^\varrho}$, $\overline{\alpha^{-\varrho}}\in Z^{(k)}$. Since $Z^{(k)}$ is a group, we get

$$\overline{\xi n}Z^{(k)}=\overline{\xi n\alpha^{-\varrho}}\cdot Z^{(k)}=\overline{\xi\alpha^{-\varrho}}\cdot\overline{n}Z^{(k)}=\overline{\eta n}Z^{(k)},$$

where $\eta=d_\varrho+d_{\varrho+1}\alpha+\cdots+d_{f-1}\alpha^{f-\varrho+1}$. This proves the Lemma.

Now we are able to prove the main theorem of this section:

Theorem 3. *Let $R(\vartheta)$ be an algebraic number field of finite degree over the field of rational numbers. Let $J[\vartheta]$ be the integral domain of algebraic integers $\in R(\vartheta)$; $\mathfrak{p}$ a prime ideal of $J[\vartheta]$, $N(\mathfrak{p})=p^f, f\geqq 1, \mathfrak{p}\|p$. Let be further $\delta=(k, p^f-1)\leqq p-1$, $s=\dfrac{p^{f(t+1)}-1}{p^f-1}\,\delta$. Suppose $a_1, a_2, \ldots, a_s$ are s elements $\in J[\vartheta]$ with $a_1\cdot a_2\cdots a_s\not\equiv 0 \pmod{\mathfrak{p}}$. Then the congruence*

$$b\equiv a_1\xi_1^k+a_2\xi_2^k+\cdots+a_s\xi_s^k \pmod{\mathfrak{p}^{t+1}}$$

has for every $b\in J[\vartheta]$ a solution with $\xi_i\in J[\vartheta]$.

Remark: In other words: under the above suppositions the equation

$$\bar{b} = \bar{a}_1 \bar{\xi}_1^k + \cdots + \bar{a}_s \bar{\xi}_s^k$$

is solvable in Z for every $\bar{b} \in Z$.[14])

Proof. For $\bar{b} = \bar{0}$ it is sufficient to choose $\xi_i = 0$. Therefore we shall suppose $\bar{b} \in Z_0$.

1. We choose the arrangement of the complexes in the relation

$$Z_0 = \bar{n}_1 Z^{(k)} + \bar{n}_2 Z^{(k)} + \cdots + \bar{n}_s Z^{(k)} \tag{30}$$

in a special way.

First take the complex $\bar{a}_1 Z^{(k)}$. Then we take the complex $\bar{c}_2 \bar{a}_2 Z^{(k)}$, where c_2 is chosen as follows. Among all numbers c_2 from (29) satisfying the condition

$$\bar{c}_2 \bar{a}_2 Z^{(k)} \subset Z_0 - \bar{a}_1 Z^{(k)} \cdot \tag{31}$$

we take those with the smallest length $l_2 \geqq 1$. From them we choose the element $c_2 = c_{02} + c_{12}\alpha + \cdots + c_{l-1,2}\alpha^{l-1}$ such that $c_{02} \not\equiv 0$ and c_{02} has the least possible positive value $\geqq 1$. According to Lemma 14 this is always possible and by Lemma 13 we have $1 \leqq c_{02} \leqq p^{t+1} - 1$.

We show now that (if $s > 1$) an element satisfying (31) really exists. According to the assumption $a_2 \not\equiv 0 \pmod{\mathfrak{p}}$, hence $\bar{a}_2 \in Z^*$.[16]) Let us multiply (30) by $\bar{a}_2 \neq \bar{0}$. We get

$$\bar{a}_2 Z_0 = \bar{n}_1 \bar{a}_2 Z^{(k)} + \bar{n}_2 \bar{a}_2 Z^{(k)} + \cdots + \bar{n}_s \bar{a}_2 Z^{(k)}.$$

Since $\bar{a}_2 \not\equiv 0 \pmod{\mathfrak{p}}$ it holds $\bar{a}_2 Z_0 = Z_0$.[17]) Hence we get

$$Z_0 = \bar{n}_1 \bar{a}_2 Z^{(k)} + \bar{n}_2 \bar{a}_2 Z^{(k)} + \cdots + \bar{n}_s \bar{a}_2 Z^{(k)}. \tag{32}$$

This is a decomposition of Z_0 modulo the complex $\bar{a}_2 Z^{(k)}$. Every summand is one of the complexes modulo $Z^{(k)}$. It follows from the equality of both

---

[14]) Theorem 1 is a special case of Theorem 3 (for $t = 0$). In this case the assumption $\mathfrak{p} \| p$ can be replaced by the weaker one $\mathfrak{p} | p$ since in this case Lemma 13 holds without the assumption $\mathfrak{p} \| p$.

At the same time Theorem 3 is a wide generalization of an important theorem used in the Waring problem. (See Landau [6], p. 289, Satz 300 or Vinogradov [11], p. 273.) This theorem is obtained by putting in Theorem 3 $f = 1$, $a_1 = a_2 = \cdots = a_s = 1$. (The condition $\delta \leqq p - 1$ is then automaticly satisfied, what enables much simpler proofs.)

[15]) According to our agreement we choose always the representant n of the class $\bar{n}$ from the set (29).

[16]) The complex $\bar{a}_2 Z^{(k)}$ is one of the cosets of the decomposition of the group Z^* modulo the subgroup $Z^{(k)}$.

[17]) This follows from the fact that $\bar{\xi} \neq \bar{\eta}$ implies $\bar{a}_2 \bar{\xi} \neq \bar{a}_2 \bar{\eta}$. For, $\bar{a}_2 \bar{\xi} = \bar{a}_2 \bar{\eta}$, i. e. $a_2 \xi = a_2 \eta \pmod{\mathfrak{p}^{t+1}}$, would imply $\mathfrak{p}^{t+1} | a_2(\xi - \eta)$. Since $\mathfrak{p} \nmid a_2$ we would have $\mathfrak{p}^{t+1} | \xi - \eta$, i. e. $\xi \equiv \eta \pmod{\mathfrak{p}^{t+1}}$, $\bar{\xi} = \bar{\eta}$, contrary to the assumption.

sides in (32) that all complexes on the right hand side are disjoint. Hence if $\bar{c}_2$ runs through all elements $\in Z_0$, $\bar{c}_2\bar{a}_2 Z^{(k)}$ gives all complexes modulo $Z^{(k)}$ and (if $s>1$) an element $\bar{c}_2$ satisfying (31) really exists.

Take now the complex $\bar{c}_3\bar{a}_3 Z^{(k)}$, where $\bar{c}_3$ is chosen as follows. We find all numbers c_3 satisfying

$$\bar{c}_3\bar{a}_3 Z^{(k)} \subset Z_0 - \bar{a}_1 Z^{(k)} - \bar{c}_2\bar{a}_2 Z^{(k)} \tag{33}$$

and having the smallest length $l_3>0$. If $s>2$ such a c_3 exists. (This can be proved analogously as above.) From all numbers c_3 of the length l_3 we choose an element

$$c_3 = c_{03} + c_{13}\alpha + \cdots + c_{f-1,3}\alpha^{f-1}$$

with $c_{03} \neq 0$, where c_{03} has the least possible positive value $\geqq 1$.

We repeat this process just s times. The last element $c_s = c_{0s} + c_{1s}\alpha + \cdots + c_{f-1,s}\alpha^{f-1}$ is chosen as follows. We find first all elements c_s of the least possible length having the property

$$\bar{c}_s\bar{a}_s Z^{(k)} \subset Z_0 - \bar{a}_1 Z^{(k)} - \bar{c}_2\bar{a}_2 Z^{(k)} - \cdots - \bar{c}_{s-1}\bar{a}_{s-1} Z^{(k)}.$$

Among them we choose an element c_s whose first coordinate $c_{0s} \neq 0$ has the least possible positive value $\geqq 1$.

The rearrangement of the decomposition (30) into complexes has the final form:

$$Z_0 = \bar{c}_1\bar{a}_1 Z^{(k)} + \bar{c}_2\bar{a}_2 Z^{(k)} + \cdots + \bar{c}_s\bar{a}_s Z^{(k)},\ c_1 = 1. \tag{34}$$

2. To prove our theorem it is sufficient to show that every element of the set

$$\bar{a}_1\bar{c}_1,\ \bar{a}_2\bar{c}_2, \ldots, \bar{a}_s\bar{c}_s,\ c_1 = 1,$$

can be written in the form

$$\bar{a}_1\bar{\xi}_1^k + \bar{a}_2\bar{\xi}_2^k + \cdots + \bar{a}_s\bar{\xi}_s^k.$$ [18])

We shall prove more. We shall show that every $\bar{a}_i\bar{c}_i$ $(1 \leqq i \leqq s)$ can be written already in the form

$$\bar{a}_i\bar{c}_i = \bar{a}_i\bar{\xi}_1^k + \cdots + \bar{a}_i\bar{\xi}_i^k,\quad \bar{\xi}_1, \ldots, \bar{\xi}_i \in Z.$$

This follows by induction. The statement is true for $i=1$ since $\bar{a}_1\bar{c}_1 = \bar{a}_1 = \bar{a}_1 \cdot 1^k$. Suppose that our statement is true for all $\bar{a}_t\bar{c}_t$, $1 \leqq t < i$. We prove it for $\bar{a}_i\bar{c}_i$. Let the element

$$c_i = c_{0i} + c_{1i}\alpha + \cdots + c_{f-1,i}\alpha^{f-1}$$

---

[18]) Since every element $\in Z_0$ arises from one of the $\bar{a}_i\bar{c}_i$ $(1 \leqq i \leqq s)$ by multiplication by a suitable k-th power.

be of the length l_i. Let us construct the complex $\overline{(c_i-1)}\bar{a}_i Z^{(k)}$ and let us consider the number

$$c_i-1=(c_{0i}-1)+c_{1i}\alpha+\cdots+c_{f-1,i}\alpha^{f-1}.$$

If $c_{01}=1$, c_i-1 has a length less then c_i. If $c_{i0}\neq 1$, c_i-1 has the same length l_i but its first coordinate is less than the first coordinate of the number c_i. In both cases (with respect to the definition of the number c_i) the complex $\overline{(c_i-1)}\bar{a}_i Z^{(k)}$ satisfies

$$\overline{(c_i-1)}\bar{a}_i Z^{(k)}\subset \bar{c}_1\bar{a}_1 Z^{(k)}+\cdots+\bar{c}_{i-1}\bar{a}_{i-1}Z^{(k)}.$$

This means: there exists an index $t\leqq i-1$ and such a number ξ_0 that $\overline{(c_i-1)}\bar{a}_i=\bar{c}_t\bar{a}_t\bar{\xi}_0^k$. By the inductive supposition we can write

$$\bar{c}_t\bar{a}_t=\bar{a}_1\bar{\xi}_1^k+\bar{a}_2\bar{\xi}_2^k+\cdots+\bar{a}_{i-1}\bar{\xi}_{i-1}^k.$$

with suitable elements $\bar{\xi}_1,\bar{\xi}_2,\ldots,\bar{\xi}_{i-1}$. Hence

$$\overline{(c_i-1)}\bar{a}_i=\bar{a}_1\overline{\xi_1\xi_0^k}+\bar{a}_2\overline{\xi_2\xi_0^k}+\cdots+\bar{a}_{i-1}\overline{\xi_{i-1}\xi_0^k},$$

i. e.

$$\bar{c}_i\bar{a}_i=\bar{a}_1\cdot\overline{\xi_1\xi_0^k}+a_2\overline{\xi_2\xi_0^k}+\cdots+\bar{a}_{i-1}\overline{\xi_{i-1}\xi_0^k}+\bar{a}_i\cdot\bar{1}^k.$$

Theorem 3 is completely proved.

IV.

Theorem 3 enables us to prove the following

Theorem 4. *Let K be the derived field of an algebraic number field $R(\vartheta)$ complete under a discrete valuation corresponding to a prime ideal $\mathfrak{p}$ of $J[\vartheta]$. Let be further*

a) $N(\mathfrak{p})=p^f$, $f\geqq 1$, $p>2$;

b) $\mathfrak{p}\|p$;

c) $k>1$, $k=k_0p^t$, $(k_0,p)=1$, $t\geqq 0$, $(k,p^f-1)\leqq p-1$;

d) $s=\dfrac{p^{f(t+1)}-1}{p^f-1}(k,p^f-1)$, $a_1,a_2,\ldots,a_{s+1}$ $s+1$ *integral elements* $\in K$ *satisfying* $a_1\cdot a_2\cdots a_{s+1}\not\equiv 0\pmod{\mathfrak{p}}$.

Then every number $b\in K$ can be written in the form

$$b=a_1\xi_1^k+a_2\xi_1^k+\cdots+a_{s+1}\xi_{s+1}^k$$

with suitable $\xi_1,\xi_2,\ldots,\xi_{s+1}\in K$.

Proof. The proof will be — to a some extent — a repetition of the proof of Theorem 2.[19]) Without loss of generality suppose b integral.

We write again

$$f(\mathbf{x}) = a_1 x_1^k + \cdots + a_s x_s^k - b$$

and use the notations from the proof of Theorem 2.

1. Suppose first $b \not\equiv 0 \pmod{\mathfrak{p}}$. According to Theorem 3 there exists a primitive vector $\mathbf{v}_1 = [\xi_{11}, \xi_{21}, \ldots, \xi_{s1}]$ such that $f(\mathbf{v}_1) \equiv 0 \pmod{\mathfrak{p}^{t+1}}$. Let be $f(\mathbf{v}_1) = f(\xi_{11}, \ldots, \xi_{s1}) = c \cdot \pi^n$, $m \geqq t+1$, $\pi^n \| f(\mathbf{v}_1)$, $c \in I$. Find a vector $[\eta_1, \eta_2, \ldots, \eta_s]$ the components of which satisfy the relation

$$c + \sum_{i=1}^{s} k_0 \left(\frac{p}{\pi}\right)^t a_i \xi_{i1}^{k-1} \eta_i \equiv 0 \pmod{\mathfrak{p}}. \tag{35}$$[19a])

This is possible since $c \not\equiv 0 \pmod{\mathfrak{p}}$ and at least one of the summands is $\not\equiv 0 \pmod{\mathfrak{p}}$. Put $\xi_{i2} = \xi_{i1} + \eta_i \cdot \pi^{m-t}$ and consider the primitive vector $\mathbf{v}_2 = [\xi_{12}, \xi_{22}, \ldots, \xi_{s2}]$. We have

$$\begin{aligned} f(\mathbf{v}_2) &= \sum_{i=1}^{s} a_i (\xi_{i1} + \eta_i \pi^{m-t})^k - b = \\ &= f(\mathbf{v}_2) + \sum_{i=1}^{s} a_i k_0 p^t \xi_{i1}^{k-1} \eta_i \pi^{m-t} + \sum_{i=1}^{s} a_i \binom{k}{2} \xi_{i1}^{k-2} \eta_i^2 \pi^{2(m-t)} + \cdots = \\ &= \pi^m \left[c + \sum_{i=1}^{s} a_i k_0 \left(\frac{p}{\pi}\right)^t \xi_{i1}^{k-1} \eta_i \right] + \sum_{i=1}^{s} a_i \xi_{i1}^{k-2} \eta_i^2 \binom{k}{2} \pi^{2(m-t)} + \cdots . \end{aligned} \tag{36}$$

The first bracket on the right is divisible by $\mathfrak{p}$ in a power equal or greater than $m+1 \geqq t+2$. According to the Lemma 4b for $p \geqq 3$, $l \geqq 2$, $m-t \geqq 1$ the expression $\binom{k}{l} \pi^{l(m-t)}$ is divisible by $\mathfrak{p}^{t+2}$. Hence the second term (and the more each of the remainig terms) is divisible at least by $\mathfrak{p}^{t+2}$. Therefore for $p \geqq 3$ it holds certainly

$$f(\mathbf{v}_2) \equiv 0 \pmod{\mathfrak{p}^{t+2}}. \tag{37}$$

Let us remark further: if moreover $m-t > 1$ then (according to lemma 4c) for $p = 2$ ($l \geqq 2$) the expression $\binom{k}{l} \pi^{l(m-t)}$ is divisible at least by

---

[19]) Theorem 2 is not merely a special case of Theorem 4. It should be noted explicitly that

a) Theorem 2 holds also in the case $\mathfrak{p}^i | p$, where $i > 1$.

b) Theorem 2 holds also for $\mathfrak{p} | 2$.

c) Theorem 2 holds also in the case *B*.

This is the true reason for which we have found it convenient to prove Theorem 2 separately.

[19a]) Note that since $\mathfrak{p} \| p$, $\mathfrak{p} \| \pi$ the quotient $\frac{p}{\pi}$ is a unit in K, hence $\frac{p}{\pi} \in I$.

$\mathfrak{p}^{t+m-t+1} = \mathfrak{p}^{m+1}$. Since $m+1 \geqq t+2$ the relation (37) holds in this case even for $p=2$.

We repeat the process used to the construction of the vector $\mathbf{v}_2$.

Let be $f(\mathbf{v}_2) = c' \cdot \pi^{m'}$, $m' \geqq t+2$, $\pi^{m'} \| f(\mathbf{v}_2)$, $c \in I$. Find a vector $[\zeta_1, \zeta_2, \ldots, \zeta_s]$ the components of which satisfy the congruence

$$c' + \sum_{i=1}^{s} k_0 \left(\frac{p}{\pi}\right)^t a_i \xi_{i2}^{k-1} \zeta_i \equiv 0 \pmod{\mathfrak{p}}.$$

Put $\xi_{i3} = \xi_{i2} + \zeta_i \pi^{m'-t}$ and consider the primitive vector $\mathbf{v}_3 = [\xi_{13}, \xi_{23}, \ldots, \xi_{s3}]$. We have

$$f(\mathbf{v}_3) = \sum_{i=1}^{s} a_i (\xi_{i2} + \zeta_i \pi^{m'-t})^k - b =$$

$$= f(\mathbf{v}_2) + \sum_{i=1}^{s} a_i k_0 p^t \xi_{i2}^{k-1} \zeta_i \pi^{m'-t} + \sum_{i=1}^{s} a_i \binom{k}{2} \xi_{i2}^{k-2} \zeta_i^2 \pi^{2(m'-t)} + \cdots =$$

$$= \pi^{m'} \left[c' + \sum_{i=1}^{s} a_i k_0 \left(\frac{p}{\pi}\right)^t \xi_{i2}^{k-1} \zeta_i \right] + \sum_{i=1}^{s} a_i \xi_{i2}^{k-2} \xi_i^2 \binom{k}{2} \pi^{2(m'-t)} + \cdots .$$

The first bracket on the right is divisible by $\mathfrak{p}$ in a power at least equal to $m'+1 \geqq t+3$. Since $m'-t \geqq 2$ we see (according to Lemma 4c) that for $p \geqq 2$, $l \geqq 2$ the expression $\binom{k}{2} \pi^{2(m'-t)}$ is divisible by $\mathfrak{p}$ in a power at least equal to $t+(m'-t)+1 = m'+1 \geqq t+3$. Hence

$$f(\mathbf{v}_3) \equiv 0 \pmod{\mathfrak{p}^{t+3}}.$$

Repeating this process we get a sequence of primitive vectors $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \ldots$ satisfying $f(\mathbf{v}_i) \equiv 0 \pmod{\mathfrak{p}^{t+i}}$.

Since the set of integers $\in I$ which are $\not\equiv 0 \pmod{\mathfrak{p}}$ is compact we can choose a subsequence which converges coordinatewise to a primitive vector $\mathbf{v}$. With respect to the continuity of the function $f(\mathbf{x})$ this vector satisfies $f(\mathbf{v}) = 0$.

This proves Theorem 4 in the case $b \not\equiv 0 \pmod{\mathfrak{p}}$ with the supplementary result that we can choose $\xi_{s+1} = 0$.

2) Suppose $b \equiv 0 \pmod{\mathfrak{p}}$. There would be possible to use the above argument if there existed a primitive vector $[\xi_{11}, \xi_{21}, \ldots, \xi_{s1}]$ satisfying

$$0 \equiv a_1 \xi_{11}^k + \cdots + a_s \xi_{s1}^k \pmod{\mathfrak{p}^{t+1}}. \tag{38}$$

We have seen in the remark to Theorem 2 that — in general — this is not the case.

Consider therefore the element $c = b - a_{s+1}$. Then $c \not\equiv 0 \pmod{\mathfrak{p}}$. According to the proof sub 1 there exist s numbers $\xi_1, \ldots, \xi_s \in K$ with

$$b - a_{s+1} = a_1 \xi_1^k + \cdots + a_s \xi_s^k.$$

Hence

$$b = a_1\xi_1^k + \cdots + a_s\xi_s^k + a_{s+1}\cdot 1^k.$$

Theorem 4 is completely proved.

It follows from the proof just given:

Theorem 4a. *Let the suppositions of Theorem 4 be satisfied with the modification that there are given only s integral elements* $a_1, \ldots, a_s \in K$ *with* $a_1 a_2 \ldots a_s \not\equiv 0 \pmod{\mathfrak{p}}$. *Then, if* (38) *has at least one non-zero solution, then every element* $b \in K$ *can be written already in the form* $b = a_1\xi_1^k + \cdots + a_s\xi_s^k$, $\xi_i \in K$.

Remark 1. Theorem 4 has been proved under the supposition $\mathfrak{p} \| p$. We show on a simple example that this supposition cannot be omitted. Let $K = R(\sqrt{-5})_{\mathfrak{p}}$, where $\mathfrak{p} = [\sqrt{-5}]$, i. e. $[p] = [5] = \mathfrak{p}^2$, $N(\mathfrak{p}) = 5$, $f = 1$. Choose $a_1 = \cdots = a_s = 1$ and $k = 5$. There exist numbers $b \in R(\sqrt{5})$ for which

$$b \equiv \xi_1^5 + \cdots + \xi_s^5 \pmod{\mathfrak{p}^2} \tag{39}$$

has no solution with integral $\xi_1, \ldots, \xi_s$ for any $s \geqq 1$. Such a number is for instance $b = \sqrt{-5}$. The complete set of representantes of the classes (mod $[\sqrt{-5}]$) is $\{0, 1, 2, 3, 4\}$. Representantes of the residue-classes (mod $\mathfrak{p}^2$) are the numbers $c_0 + c_1\sqrt{-5}$ ($c_0, c_1 = 0, \ldots, 4$). The elements of the set $Z^{(5)}$ are $Z^{(5)} = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ (fifth power residues (mod $\mathfrak{p}^2$)). If (39) were solvable for $b = \sqrt{-5}$ it would be possible to write $\sqrt{-5} \equiv \sum_{i=1}^{s} d_i \pmod{[5]}$, $0 \leqq d_i < 5$, i. e. $\sqrt{-5} - d \equiv 0 \pmod{[5]}$, where $0 \leqq d < 5$. This is impossible since $\frac{\sqrt{-5} - d}{5}$ is not an algebraic integer $\in R(\sqrt{-5})$.

Let us look for where the proof of Theorem 4 fails in the case $\mathfrak{p}^i | p$, $i \geqq 2$. Lemma 13 does not hold.[20]) But it can be proved (see for instance O. *Ore* [8], p. 58) that it is always possible to find a number γ satisfying (11) so that every residue $\omega \pmod{\mathfrak{p}^a}$ (for $a \geqq e$ where $\mathfrak{p}^e \| p$) can be written in the form $\omega = D(\gamma)$, where $D(\gamma)$ is a polynomial in γ with rational integral coefficients. (Briefly: τ can be eliminated from Lemma 3.)[21]) Hence there would be possible to introduce the notions of the length and coordinates. But this γ (and this is essential!) cannot be written — in general — in the form $\gamma \equiv \beta^k \pmod{\mathfrak{p}^{i+1}}$. Therefore we cannot say that every complex $\bar{n}Z^{(k)}$ con-

[20]) F. i. in our example it is not true that every residue $\omega \pmod{\mathfrak{p}^2}$ is of the form $\omega \equiv d_0 \pmod{\mathfrak{p}^2}$ where $d_0 = 0, 1, \ldots, 24$. (Only 5 of these residues are different.)

[21]) In our example it is sufficient to choose $\gamma = \sqrt{-5}$. Then the complete system of residues (mod $\mathfrak{p}^2$) can be written in the form $c_0 + c_1\gamma$ ($c_0, c_1 = 0, 1, \ldots, 4$).

tains an element $c_0+c_1\alpha+c_2\alpha^2+\cdots$ with $c_0\not\equiv 0$, i. e. Lemma 14 does not hold.[22]) The induction used in the proof of Theorem 3 cannot be applied.

Remark 2. Theorem 4 was proved under the supposition $p>2$. Consider now a prime ideal $\mathfrak{p}$ with $N(\mathfrak{p})=2^f, f\geqq 1$. Theorem 3 holds but is not sufficient to the proof of a theorem analogous to Theorem 4.

For, if $\mathfrak{p}|2$ we have $\mathfrak{p}^{t+1}\left\|\frac{k(k-1)}{2}\pi^2\right.$ so that for $m-t=1$ the equation (36) implies instead of (37) only

$$f(\mathbf{v}_2)\equiv\sum_{i=1}^{s}a_i\xi_{i1}^{k-2}\eta_i^2\binom{k}{2}\pi^2 \pmod{\mathfrak{p}^{t+2}}$$

and the right hand side is — in general — $\not\equiv 0 \pmod{\mathfrak{p}^{t+2}}$.

This can really take place as an example in the rational 2-adic field shows. Choose $f(\mathbf{x})=x_1^2+x_2^2+x_3^2-7$. Here $\mathfrak{p}=p=2, k=2$, i. e. $t=1, s=3$. The vector $\mathbf{v}_1=[1,1,1]$ satisfies (in accordance with Theorem 3) $f(\mathbf{v}_1)\equiv 0 \pmod{\mathfrak{p}^{t+1}=2^2}$. We have $f(\mathbf{v}_1)=-1\cdot 2^2$. The equation (35) is of the form

$$-1+\eta_1+\eta_2+\eta_3\equiv 0 \pmod 2. \tag{40}$$

This equation is soluble. But constructing the vector

$$\mathbf{v}_2=[1+2\eta_1, 1+2\eta_2, 1+2\eta_3]$$

we get

$$f(\mathbf{v}_2)=4(-1+\eta_1+\eta_2+\eta_3)+4(\eta_1^2+\eta_2^2+\eta_3^2),$$

i. e. $f(\mathbf{v}_2)\equiv 4(\eta_1^2+\eta_2^2+\eta_3^2) \pmod{2^3}$ and for η_i satisfying (40) we have clearly $\eta_1^2+\eta_2^2+\eta_3^2\equiv 1\not\equiv 0 \pmod 2$, whence $f(\mathbf{v}_2)\not\equiv 0 \pmod{2^3}$.[23])

This shows that Theorem 4 cannot hold in general for $p=2$, at least not in the case if the number s keeps the meaning introduced above.

But one proves immediately the validity of the following assertion.

If for some s *and* $a_1a_2\ldots a_s\not\equiv 0 \pmod{\mathfrak{p}}$ *the congruence*

$$b\equiv a_1\xi_{10}^k+\cdots+a_s\xi_{s_0}^k \pmod{\mathfrak{p}^{t+2}}$$

has a non-zero solution $(\xi_{10},\ldots,\xi_{s_0})$, *then*

$$b=a_1\xi_1^k+\cdots+a_s\xi_s^k$$

is soluble in K *even in the case* $\mathfrak{p}|2$.

---

[22]) In the case $R(\sqrt{-5})$, $\mathfrak{p}=[\sqrt{-5}]$, $k=5$ there exist seven complexes: $\{0\}$, $Z^{(5)}=\{1,2,3,4\}$, $\{1+\sqrt{-5}, 2+2\sqrt{-5}, 3+3\sqrt{-5}, 4+4\sqrt{-5}\}$, $\{1+2\sqrt{-5}, 2+4\sqrt{-5}, 3+\sqrt{-5}, 4+3\sqrt{-5}\}$, $\{2+\sqrt{-5}, 4+2\sqrt{-5}, 1+3\sqrt{-5}, 3+4\sqrt{-5}\}$, $\{1+4\sqrt{-5}, 2+3\sqrt{-5}, 3+2\sqrt{-5}, 4+\sqrt{5}\}$, $\{\sqrt{-5}, 2\sqrt{-5}, 3\sqrt{-5}, 4\sqrt{-5}\}$.

In the last complex there does not exist an element with the first coordinate $\neq 0$.

[23]) It is clear, of course, in advance that $\xi_1^2+\xi_2^2+\xi_3^2\equiv 7 \pmod 8$ is not soluble with integral ξ_1, ξ_2, ξ_3.

The proof follows from the fact that for $\varrho > 1$ Lemma 4 *c*) holds also in the case $p = 2$. In the step from the congruence (mod p^{t+2}) to the congruence (mod p^{t+3}) we get always (i. e. also for $p|2$) a linear congruence which is soluble.

Bibliography.

[1] R. Brauer, A note on systems of homogeneous algebraic equations, *Bulletin Amer. Math. Soc.*, **51** (1945), 749—755.

[2] C. Chevalley, Démonstration d'une hypothèse de M. Artin, *Abhandlungen Math. Sem. d. Hansischen Univ.*, **11** (1935), 73—75.

[3] V. B. Demyanov, On cubic forms in discretely normed fields (russian), *Doklady Akad. Nauk. SSSR*, **74** (1950), 889—891.

[4] H. Hasse, Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlenkörper, *Journal f. d. reine u. angew. Math.*, **153** (1924), 113—130.

[5] B. W. Jones, *The Arithmetic Theory of Quadratic Forms.* (Baltimore, 1950).

[6] E. Landau, *Vorlesungen über Zahlentheorie*, I. Bd. (Leipzig, 1927).

[7] D. J. Lewis, Cubic homogeneous polynomials over p-adic number fields, *Annals of Math.*, **56** (1952), 473—478.

[8] O. Ore, Les corps algébriques et la théorie des ideaux, *Mémorial des sciences mathématiques*, LXIV (Paris, 1934).

[9] Št. Schwarz, On Waring's problem for finite fields, *Quarterly Journal of Math.* (Oxford), **19** (1948), 123—128.

[10] Št. Schwarz, On universal forms in finite fields, *Časopis pěst. mat. fys.*, **75** (1950), 45—50.

[11] I. M. Vinogradov, *Collected papers* (russian) (Moscow, 1952).

(*Received June 8, 1955.*)